Security

Jim Dieudonne and Jim Griner

Security
Key R&T Issues

- Identify key research and technology issues of both near-term (now to 2010) and far-term (beyond 2010) impact.
  - With proper Systems Engineering, near-term and far-term issues will be revealed (requirements definition/identification, risk assessment).
    - Near-term
      - Address policy and regulatory issues that can or should be changed.
        - » For example, IPvX utilization for CNS.
        - » FAA has the ability to impact the near-term solutions.
      - Protection of all aviation networks and databases from attack.
    - Long-term
      - NASA can best impact the long-term technology solutions.
      - Autonomous oversight and identification of ‘abnormal’ behavior to take control.
      - New sensors to detect uncooperative entities.
      - Next GPS, Communication and security of those systems.

Security
Current Work

- Identify known work being done to address R&T issues in the topical area being discussed, and organizations doing the work.
  - See presentations from dedicated conference Security and Surveillance sessions.
  - Assimilation and networking of current systems and services.
    - Implementation is easier said than done.
  - Does ATA have working groups in this area? RTCA started to create a working group in this area, but it was postponed. Too public?
    - Leaked information is an issue.
  - FAA NAS Security Architecture and Vulnerability Assessment
  - SARPs v3 has security in it (at least for data).
  - Protected DoD systems may be a good starting point for consideration (Military frequency hopping ability).

Security
Unaddressed Issues

- Identify issues not being addressed by any known R&T effort, as well as areas where current work is inadequate or underfunded.
  - What are total operational requirements for system-wide (airborne & not) aviation security? (Level of protection)
    - Look at mitigation instead of prevention. (Detecting threat (terrorists or other realistic vulnerabilities), identifying targets, sending alerts.)
  - For implemented ICNS, what about new firewall technologies, cyber intrusion (infrastructure)?
    - IP application
  - What about authentication?
    - Human recognition biometrics.
    - Protecting privacy and guarding identities while still providing securities.
  - Leveraging military solutions in civil aviation environment.
    - Affordability?
  - Who's responsible FOR civil aviation environment if it is attacked or setting security requirements? (FAA, DoD, TSA)?
    - Who's domain is the 'cropduster'?
  - Corruption of databases and jamming, shutting down GPS's?
  - ILS/LAAS safeguards?
  - Retaining situational awareness with new data link technologies.

Security Priorities

- Prioritize the key R&T issues needing attention.
  - Determine the scope of CNS security.
    - From GA to Military.
  - Who is responsible (FAA, DoD, LE, TSA)?
  - Cyber protection (ground and air).
  - Utilize current technologies where possible to improve security.

Security
Recommended Approach

- Recommend approaches to address the key R&T needs, organizations which might address these needs, needed collaborations or cooperative efforts, etc.
  - Systems engineering approach to security.
  - Revisit decommissioning of current CNS tools until a multi-layered security system can be designed.
  - NASA should participate, where practical, in the studies on systems engineering (requirements, vulnerabilities, risk assessment etc.) and current system applications then decide where to perform R&D for future systems.